CentER

Discussion paper

No. 2001-83

THE HERMITIAN TWO-GRAPH AND ITS CODE

By Willem H. Haemers and Elisabeth Kuijken

November 2001

ISSN 0924-7815

The Hermitian two-graph and its code

Willem H. Haemers
Department of Econometrics and Operations Research
Tilburg University
5000 LE Tilburg, The Netherlands
Haemers@kub.nl

Elisabeth Kuijken*
Department of Pure Mathematics and Computer Algebra
Ghent University
Galglaan 2, B-9000 Ghent, Belgium
ekuijken@cage.rug.ac.be

Abstract

The two-graph code of the Hermitian two-graph $\mathcal{H}(q)$ is investigated. By use of this code we show that if $q \equiv 3 \pmod 8$ there exists no strongly regular graph with valency $q^2(q-1)/2$ in the switching class corresponding to $\mathcal{H}(q)$. For $q = 5$ the code is worked out in detail. We generate the weight enumerator and give an account for the code words of several weights. Here it follows that there is a unique regular graph with valency 50 in the switching class.

Keywords: discrete mathematics, finite geometry, strongly regular graph, error correcting code. Mathematics Subject Classification: 05E30, 51E20, 94B05. JELcode: C0.

*The second author is a Research Assistant of the Fund for Scientific Research - Flanders (Belgium) (F.W.O.). Most of this research was done during a visit to Tilburg University (The Netherlands) and was supported by a Marie Curie Fellowship of the European Community programme MARIE CURIE TRAINING SITES: ENTER under contract number HPMT-CT-00-00134, reference number of the fellow HPMT-GH-00-00134-17.

1 Introduction

A two-graph can be seen as a class of graphs on a common vertex set that are equivalent under an operation called *switching* (see section 2). In case of a regular two-graph one wonders whether there exists a regular graph in such a class. If so, that graph is necessarily strongly regular. There are only two candidates k_f and k_g (say) for the valency of such a graph. For the Hermitian two-graph $\mathcal{H}(q)$ (q is an odd prime power) such graphs were known to exist for one of the valencies $k_g = q(q^2+1)/2$ for all q, but not for $k_f = q^2(q-1)/2$, $q > 5$. For $q = 3$ there is no graph with valency $k_f = 9$, but for $q = 5$ there is one with $k_f = 50$. We prove that for the valency k_f there is no such graph in $\mathcal{H}(q)$ if $q \equiv 3 \pmod 8$, and that the one for $q = 5$ is unique up to isomorphism. For the Ree two-graph $\mathcal{R}(q)$ (q is an odd power of 3) we show a similar result. To do so we use a binary code related to the two-graph, called the *two-graph code* (the name is introduced in [9], but the concept was used earlier in [8] and [2]). An important tool is Theorem 4.1 cited from [9], which relates the code to graphs in the switching class.

Much attention is given to the case $q = 5$. For that case we give an explicit description of the mentioned graph in $\mathcal{H}(5)$ with valency $k_f = 50$. We compute the weight enumerator of the two-graph code, and give a description of the words of several of the occuring weights. Some of these words are explained by using a different construction of $\mathcal{H}(5)$, based on the Hoffman-Singleton graph.

2 Two-graphs

This section gives a brief introduction to two-graphs; we recommend [15] and [18] for more information. The reader is assumed to be familiar with *(strongly regular) graphs*, their $(0, 1)$ *adjacency matrices* and their *eigenvalues*. A strongly regular graph with parameters v, k, λ and μ will be abbreviated to srg (v, k, λ, μ).

Consider a graph Γ with vertex set Ω and let $\{\Omega_1, \Omega_2\}$ be a partition of Ω. Interchange edges and non-edges between vertices of Ω_1 and vertices of Ω_2, while (non-)edges inside Ω_1 and inside Ω_2 are left unchanged. A new graph Γ' arises; the construction of Γ' from Γ is called *(Seidel) switching* with respect to the partition $\{\Omega_1, \Omega_2\}$ of Ω, and Γ and Γ' are said to be *switching equivalent*. Switching equivalence is indeed an equivalence relation; the classes are called *switching classes*.

A *two-graph* is a pair (Ω, Δ) of a finite *vertex set* Ω and a set Δ of unordered triples from Ω called *coherent triples*, such that every set of four vertices contains an even number of coherent triples. Let Γ be a graph with vertex set Ω and define Δ as the set of unordered triples of vertices containing an odd number of edges. Then (Ω, Δ) is a two-graph, and we say that Γ is a graph *in* (Ω, Δ). It easily follows that a graph Γ' is switching equivalent to Γ if and only if Γ' and Γ are in the same two-graph. Let ∇

denote the set of non-coherent unordered triples from Ω. Then (Ω, ∇) is also a two-graph, called the *complement* of (Ω, Δ) (sometimes denoted by $\overline{(\Omega, \Delta)}$). If the graph Γ is in (Ω, Δ), then clearly $\overline{\Gamma}$, the complement of Γ, is in (Ω, ∇). For a fixed vertex $u \in \Omega$ there is a unique graph Γ_u in (Ω, Δ) where u is an isolated vertex.

A two-graph (Ω, Δ) is *regular* if every pair of vertices is contained in a constant number a of coherent triples. The numbers $n := |\Omega|$ and a are called the *parameters* of the regular two-graph (Ω, Δ). Regular two-graphs are closely related to strongly regular graphs. Let (Ω, Δ) be a regular two-graph with parameters n and a, and let Γ_u be the graph in (Ω, Δ) for which u is an isolated vertex. The graph Γ obtained from Γ_u by deleting u is called the *descendant* of (Ω, Δ) with respect to u. It follows that Γ is an $\mathrm{srg}\,(n-1, a, (3a-n)/2, a/2)$. And conversely, the switching class of any $\mathrm{srg}\,(v, k, \lambda, \mu)$ with $k = 2\mu$ extended with an isolated vertex is a regular two-graph with parameters $v+1$ and k.

Let (Ω, Δ) be a regular two-graph whose descendants have eigenvalues k, r and s with multiplicity 1, f and g, respectively. Then $k = -2rs$. Suppose there exists a regular graph Γ' in (Ω, Δ). Then Γ' is strongly regular with the same restricted eigenvalues r and s as the descendants. For the valency of Γ' just two values are possible: $k_f := -(2s+1)r$ and $k_g := -(2r+1)s$.

Automorphisms of two-graphs are defined in the usual way. One easily sees that a two-graph admitting an automorphism group which acts doubly transitively on the vertex set must be regular.

3 Regular partitions

Let A be a symmetric real $n \times n$ matrix and let $\{X_1, \ldots, X_d\}$ be a partition of the index set $\{1, \ldots, n\}$ of the rows and columns of A. Then, after an appropriate permutation of the rows and the corresponding columns, A can be written as

$$A = \begin{bmatrix} A_{11} & \ldots & A_{1d} \\ \vdots & & \vdots \\ A_{d1} & \ldots & A_{dd} \end{bmatrix},$$

where A_{ij} is the submatrix of A obtained by restricting the index set of the rows to X_i and the index set of the columns to X_j. Let b_{ij} denote the average of the row sums in A_{ij}, $i, j \in \{1, \ldots, d\}$. The matrix $B := (b_{ij})_{1 \le i,j \le d}$ is called the *quotient matrix* of A with respect to the partition. If for all i and j in $\{1, \ldots, d\}$ all row sums in A_{ij} are equal to b_{ij}, the partition is said to be *regular* (or *equitable*).

Lemma 3.1 *Let A be the adjacency matrix of a strongly regular graph with eigenvalues k (the valency), r and s ($r > s$). Let $\{X_1, X_2\}$ be a partition of the vertex set with* *quotient matrix*

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

1. $b_{11} + b_{12} = b_{21} + b_{22} = k$, $b_{12}|X_1| = b_{21}|X_2|$.
2. $s \leq b_{11} + b_{22} - k \leq r$.
3. *Equality holds on the left or the right hand side of 2 if and only if the partition is regular.*

Proof. Statement 1 is obvious. The eigenvalues of B are k (the row sum) and $b_{11} + b_{22} - k$. Now eigenvalue interlacing ([7], Theorem 3.5) gives 2 and the 'only if' part of 3. The 'if' part follows from the fact that in case of a regular partition the eigenvalues of B are also eigenvalues of A. But in A there are just two candidates r and s for the eigenvalue $b_{11} + b_{22} - k$. □

Lemma 3.2 *Let Γ be a descendant of a regular two-graph (Ω, Δ). Let A be the adjacency matrix of Γ and let k, r and s be its eigenvalues, where k is the valency of Γ.*

1. *There exists a regular graph in (Ω, Δ) with valency $k_f = -(2s+1)r$ if and only if A admits a regular partition $\{X_1, X_2\}$ with $|X_1| = k_f$ for which the left hand inequality in 2 of Lemma 3.1 is tight.*
2. *There exists a regular graph in (Ω, Δ) with valency $k_g = -(2r+1)s$ if and only if A admits a regular partition $\{X_1, X_2\}$ with $|X_1| = k_g$ for which the right hand inequality in 2 of Lemma 3.1 is tight.*

In both cases the regular graph in (Ω, Δ) is obtained by adding an isolated vertex to Γ and switching with respect to X_1.

The proof of Lemma 3.2 is straigtforward. The partitions occurring in this lemma are called *switch partitions*. Lemmas 3.1 and 3.2 can be of help in checking whether a partition is a switch partition. Suppose a descendant Γ of a regular two-graph has a subgraph Γ_f of size k_f and average valency at most $s(1-r)$. Then by 1 and 2 of Lemma 3.1 the average valency equals $s(1-r)$, by 3 of Lemma 3.1 the partition into the vertices of Γ_f and the remaining vertices of Γ is regular, and by Lemma 3.2 the partition is a switch partition. An analogous remark holds for a subgraph Γ_g of Γ of size k_g and average valency at least $r(1-s)$.

4 Two-graph codes

Suppose A is a $(0,1)$ matrix of size $m \times n$. The (binary) code C_A of A is defined as the subspace of $\mathbf{F}_2^n$ generated by the rows of A. The dimension of C_A is the 2-rank of A.

The code of a graph Γ is the code C_A of its adjacency matrix A. It can be proved (see for example [9]) that the 2-rank of a symmetric integral matrix with zero diagonal, and hence the dimension of the code of a graph, is always even.

Suppose that the adjacency matrix A of a graph has a regular partition $\{X_1, X_2\}$ with quotient matrix

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

By taking the sum of the rows (mod 2) of one part of the partition we see that the characteristic vector of X_i ($i \in \{1,2\}$) is in the code C_A if $b_{i,1}$ is odd and $b_{3-i,1}$ is even, or if $b_{i,2}$ is odd and $b_{3-i,2}$ is even.

Let (Ω, Δ) be a two-graph, let $u \in \Omega$ and and let A_u be the adjacency matrix of Γ_u. Then the *(two-graph) code* of (Ω, Δ) is the code $C := C_{A_u+J} = C_{A_u} + \langle \underline{1} \rangle$, that is, the code generated by the rows of A_u and the all-one vector $\underline{1}$. In [9] it is shown that the two-graph code does not depend on the choice of u and that an automorphism of the two-graph is also an automorphism of the code. The following theorem from [9] gives the relation between the codes of a regular two-graph, a descendant and a regular graph in the two-graph.

Theorem 4.1 *Let (Ω, Δ) be a regular two-graph with two-graph code C. Assume that Γ is a regular graph with valency k in (Ω, Δ). So Γ is strongly regular; let k, r and s be its eigenvalues. Take $u \in \Omega$ and let A_u and A be the adjacency matrices of Γ_u and Γ, respectively. Assume that $\{\Omega_1, \Omega_2\}$ with $u \in \Omega_2$ is the partition of Ω by which Γ_u is switched to Γ, and let χ denote the characteristic vector of Ω_1. Then one of the following holds.*

1. $C_A + \langle \underline{1} \rangle = C_{A_u} + \langle \underline{1} \rangle = C,\ \ \underline{1} \notin C_A,\ \ \chi \in C_{A_u},$
   $\dim C_A = \dim C_{A_u} = \dim C - 1.$
2. $C_A = C_{A_u} + \langle \underline{1} \rangle + \langle \chi \rangle = C + \langle \chi \rangle,\ \ \underline{1} \in C_A,\ \ \chi \notin C_{A_u},$
   $\dim C_A = \dim C_{A_u} + 2 = \dim C + 1.$

If k is even and $r+s$ is odd, then 1 holds. If $k \equiv 2 \pmod 4$ and $r+s$ is even, or k is odd, then 2 holds.

5 The Hermitian two-graph $\mathcal{H}(q)$

Taylor's description [17] of the *Hermitian two-graph* (also known as the *unitary two-graph*) reads as follows. Let q be an odd prime power, H a non-degenerate Hermitian form in $\mathrm{PG}(2, q^2)$ and $\mathcal{U}$ the corresponding Hermitian curve. Define Δ to be the set of triples $\{x, y, z\}$ from $\mathcal{U}$ for which $H(x,y)H(y,z)H(z,x)$ is a square in $\mathbf{F}_{q^2}$ if $q \equiv -1 \pmod 4$, a non-square if $q \equiv 1 \pmod 4$. Then $\mathcal{H}(q) := (\mathcal{U}, \Delta)$ is a regular two-graph with parameters $n = q^3 + 1$ and $a = (q-1)(q^2+1)/2$. Its automorphism group $\mathrm{P\Gamma U}_3(q^2)$ acts doubly transitively on $\mathcal{U}$. The descendant $\mathcal{H}'(q)$ of $\mathcal{H}(q)$ with respect to any vertex u is called the *Hermitian graph* (also known as *Taylor's graph*), and is an

$$\mathrm{srg}\left(q^3, (q-1)(q^2+1)/2, (q-1)^3/4 - 1, (q-1)(q^2+1)/4\right)$$

with eigenvalues $k = (q-1)(q^2+1)/2$, $r = (q-1)/2$ and $s = -(q^2+1)/2$ and multiplicities 1, $(q-1)(q^2+1)$ and $q(q-1)$, respectively.

The two possibilities for the valency of a regular graph in $\mathcal{H}(q)$ are $k_f = q^2(q-1)/2$ and $k_g = q(q^2+1)/2$. By switching of $\Gamma_u := \mathcal{H}'(q) \cup \{u\}$ with respect to the set of points different from u on the union of $(q^2+1)/2$ lines of the Hermitian unital through u, an

$$\mathrm{srg}\left(q^3+1, q(q^2+1)/2, (q^2+3)(q-1)/4, (q^2+1)(q+1)/4\right)$$

is obtained; in fact there are many mutually non-isomorphic strongly regular graphs with these parameters in $\mathcal{H}(q)$, see [10]. It is known that $k_f = q^2(q-1)/2$ does not occur for $q = 3$, but it does for $q = 5$ (see section 6). One of the purposes of this paper is to settle the existence question for bigger q, hoping for a positive answer for some q. Unfortunately we only have non-existence results. First we need a result from [2].

Proposition 5.1 *If $q \equiv 1 \pmod 4$, the two-graph code of $\mathcal{H}(q)$ has dimension $q^2 - q + 1$. If $q \equiv 3 \pmod 4$, the two-graph code of $\overline{\mathcal{H}(q)}$ has dimension $q^2 - q + 1$.*

The proposition has a direct proof if $q \equiv 1 \pmod 4$, but if $q \equiv 3 \pmod 4$ the proof is based on a result from Landazuri and Seitz [12] which states that a non-trivial representation of $\mathrm{P\Gamma U}_3(q^2)$ over $\mathbf{F}_2$ has degree at least $q^2 - q$.

Theorem 5.2 *For $q \equiv 3 \pmod 8$ the Hermitian two-graph $\mathcal{H}(q)$ contains no regular graph with valency $k_f = q^2(q-1)/2$.*

Proof. Assume that Γ with adjacency matrix A is a regular graph of valency k_f in $\mathcal{H}(q)$. Then the complement $\overline{\Gamma}$ of Γ is a regular graph with valency $\overline{k_f} := q^2(q+1)/2$ in $\overline{\mathcal{H}(q)}$. The eigenvalues of $\overline{\Gamma}$ are $\overline{k_f}$, $\overline{r} = (q^2-1)/2$ and $\overline{s} = -(q+1)/2$. If $q \equiv 3 \pmod 8$, then $\overline{r}$ and $\overline{s}$ are even and $\overline{k_f} \equiv 2 \pmod 4$. By Theorem 4.1 it follows that $\dim C_{\overline{A}} = \dim \overline{C} + 1$, where $\overline{C}$ denotes the two-graph code of $\overline{\mathcal{H}(q)}$. By proposition 5.1 $\dim C_{\overline{A}} = q^2 - q + 2$. It can be calculated that the eigenvalue $\overline{s}$ has multiplicity $q(q^2 - q + 1)$, and hence

$$\dim C_{\overline{A}} = \text{2-rank}(\overline{A}) = \text{2-rank}(\overline{A} - \overline{s}I) \leq \mathrm{rank}(\overline{A} - \overline{s}I) = q^2 - q + 1,$$

a contradiction. Therefore Γ cannot exist. □

The *Ree two-graph* $\mathcal{R}(q)$, $q = 3^{2e+1}$, $e \in \mathbf{N}$ (see Taylor [17]), is defined on the points of the Ree unital and has the same parameters as the Hermitian two-graph $\mathcal{H}(q)$; its automorphism group is the Ree group $R(q)$. In [12] it is also proved that a non-trivial representation of the Ree group $R(q)$ over $\mathbf{F}_2$ has degree at least $q^2 - q$. Therefore the argument above also applies for the Ree two-graph. Since $q = 3^{2e+1} \equiv 3 \pmod 8$ we have:

Theorem 5.3 *The Ree two-graph $\mathcal{R}(q)$ contains no regular graph with valency $k_f = q^2(q-1)/2$.*

Note that the Ree two-graph contains a regular graph with valency $k_g = q(q^2+1)/2$. It is constructed by a similar method as in the Hermitian case, namely by switching the descendant of $\mathcal{R}(q)$ extended with an isolated vertex u with respect to the set of points different from u on the union of $(q^2+1)/2$ lines of the Ree unital through u.

6 Regular graphs in $\mathcal{H}(5)$

For $q = 5$ there exists a description of $\mathcal{H}(5)$ in terms of the Hoffman-Singleton graph (see section 8). It was J.-M. Goethals who observed that this approach gives an srg$\,(126, 50, 13, 24)$ in the switching class of $\mathcal{H}(5)$. So for $q = 5$ there exists a graph in $\mathcal{H}(q)$ with degree $k_f = q^2(q-1)/2$. In this section we give an explicit description of a switching set S in the descendant of $\mathcal{H}(5)$ that leads to Goethals' graph.

Let the Hermitian form defining $\mathcal{H}(5)$ be given by $H(X,Y) = X_0Y_0^5 + X_1Y_2^5 + X_2Y_1^5$. If i is an element of $\mathbf{F}_{25}$ such that i^2 is equal to 2, which is a non-square in $\mathbf{F}_5$, then any element of $\mathbf{F}_{25}$ can be written as $a + bi$ for some $a, b \in \mathbf{F}_5$. This implies that the corresponding Hermitian curve is the set

$$\mathcal{U} = \{(0,1,0)\} \cup \{(a+bi, (2a^2+b^2)+di, 1) \mid a,b,d \in \mathbf{F}_5\}.$$

Suppose that $\mathcal{H}'(5)$ is the descendant of $\mathcal{H}(5)$ with respect to $u := (0,1,0)$. Then each vertex of $\mathcal{H}'(5)$ can be represented by a triple (a,b,d) from $\mathbf{F}_5^3$. It follows straightforwardly (see [16]) that two triples (a,b,d) and (a',b',d') are adjacent whenever

$$\left((a-a')^2 - 2(b-b')^2\right)^2 + 2(a'b - b'a + d - d')^2 = \pm 2.$$

The mentioned switching set S can be described in terms of triples from $\mathbf{F}_5^3$ by $S = S_1 \cup S_2$, where

$$\begin{aligned} S_1 &= \{(a,0,\pm 1) \mid a \in \mathbf{F}_5\}, \\ S_2 &= \{(a,b,\pm 2 - ab) \mid a \in \mathbf{F}_5,\ b \in \mathbf{F}_5 \setminus \{0\}\}. \end{aligned}$$

The elements of the automorphism group $\mathrm{P\Gamma U}_3(25)$ of $\mathcal{H}(5)$ can be written as $M \circ \sigma$, where M is an element of $\mathrm{PGU}_3(25)$ and can be represented by a 3×3 unitary matrix, and σ is an automorphism of $\mathbf{F}_{25}$ and hence is either the identity or the involution $\tau : x \mapsto x^5$. A general element of the stabilizer $\mathrm{P\Gamma U}_3(25)_u$ of the vertex u in $\mathrm{P\Gamma U}_3(25)$, and hence of the automorphism group of $\mathcal{H}'(5)$, is of the form

$$\begin{bmatrix} z & 0 & -zx^5 \\ x & 1 & y \\ 0 & 0 & z^6 \end{bmatrix} \circ \sigma,$$

where $z \in \mathbf{F}_{25} \setminus \{0\}$, $(x, y, 1) \in \mathcal{U} \setminus \{u\}$ and σ is an automorphism of $\mathbf{F}_{25}$. Consider the subgroup H of $\mathrm{P\Gamma U}_3(25)_u$ generated by

$$\varphi := \begin{bmatrix} 1 & 0 & 4 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}, \theta := \begin{bmatrix} 4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \tau \text{ and } \psi := \begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix} \circ \tau.$$

The elements φ, θ and ψ have order 5, 2 and 4, respectively, and preserve S_1 and S_2. One easily verifies that $\theta \circ \varphi = \varphi^4 \circ \theta$, $\psi \circ \varphi = \varphi^2 \circ \psi$ and $\theta \circ \psi = \psi \circ \theta$. Therefore the order of H equals 40. It follows by straightforward calculations that any element of $\mathrm{P\Gamma U}_3(25)_u$ stabilizing S must stabilize S_1. Moreover, exactly four elements of $\mathrm{P\Gamma U}_3(25)_u$ stabilize S and the vertex $(0, 0, 1) \in S_1$. As a consequence the stabilizer of S in $\mathrm{P\Gamma U}_3(25)_u$ has order at most 40, and hence is equal to H.

Proposition 6.1 *Switching of $\mathcal{H}'(5) \cup \{u\}$ with respect to the set S described above produces an* srg$(126, 50, 13, 24)$ *in $\mathcal{H}(5)$.*

Proof. By Lemma 3.1 it suffices to show that S induces a regular subgraph of degree 13 in $\mathcal{H}'(5)$. One easily checks that H acts transitively on S_1 and S_2; this means that we only have to calculate the degree for $(0, 0, 1)$ and $(0, 1, 2)$. For the first vertex we need to count the number of solutions of

$$(a^2 - 2b^2)^2 + 2(d - 1)^2 = \pm 2 \text{ with } (a, b, d) \in S.$$

We find one solution in S_1 and twelve in S_2. For the second vertex we count solutions in S of

$$(a^2 - 2(b - 1)^2)^2 + 2(d - a - 2)^2 = \pm 2 \text{ with } (a, b, d) \in S,$$

and find three solutions in S_1 and ten in S_2. So both vertices have degree 13. □

We tried to generalize S to larger $q \equiv 1 \bmod 4$ but failed. The obvious generalization would be to replace ± 1 by 'a non-zero square' and ± 2 by 'a non-square' in the above definition of S. This indeed gives a subset with the right number of vertices, but with too many edges (at least for $q = 9$ and $q = 13$). We also tried many variations without luck. We now have the feeling that the case $q = 5$ is special.

weight	C_A	C
0	1	1
36	259	525
42	1380	2250
48	3675	7875
50	8568	18900
52	4725	7875
54	52360	110250
56	98280	189000
58	95760	189000
60	140238	286650
62	120960	236250

weight	C_A	C
64	115290	236250
66	146412	286650
68	93240	189000
70	90720	189000
72	57890	110250
74	3150	7875
76	10332	18900
78	4200	7875
84	870	2250
90	266	525
126	0	1

Table 1: Weight distributions of the codes C_A of $\mathcal{H}'(5)$ and C of $\mathcal{H}(5)$.

7 The code of $\mathcal{H}(5)$

The weight enumerator of the code C_A of the Hermitian graph $\mathcal{H}'(5)$ with adjacency matrix A has been generated by computer using the software from [9]. From this the weight enumerator of the two-graph code C of $\mathcal{H}(5)$ immediately follows, since the number of words of weight w in C equals the number of words of weight w or $126 - w$ in C_A.

Both weight enumerators are given in Table 1. Using MacWilliams' Theorem, we also computed the weight enumerator of the dual code $C^\perp$ of C, which we give in Table 7. In [2] it is proved that $C^\perp$ is the binary code of the corresponding Hermitian unital. More precisely, if N is the block-point incidence matrix of the Hermitian unital in $\mathrm{PG}(2, 25)$, then $C^\perp = C_N$. From Table 7 we see that the number of words of weight 6 in $C^\perp$ equals 21525. Now take a coherent 6-set in $\mathcal{H}(5)$ (that is a set of six vertices of which all unordered triples are coherent). Suppose $\mathcal{H}'(5)$ is the descendant of $\mathcal{H}(5)$ with respect to a vertex u of this coherent 6-set. Then the remaining five vertices form a clique in $\mathcal{H}'(5)$. The size of the clique meets the bound of Delsarte, which implies that every vertex outside the clique is adjacent to exactly two vertices of the clique (see for example [1], Proposition 1.3.2). Let A_u be the adjacency matrix of $\mathcal{H}'(5) \cup \{u\}$; then the rows of $A_u + J$ corresponding to u and the vertices of the 5-clique in $\mathcal{H}'(5)$ sum up to $\underline{0}$. This implies that the coherent 6-set in $\mathcal{H}(5)$ corresponds to a code word in $C^\perp$ of weight 6. But the number of coherent 6-sets in $\mathcal{H}(5)$ equals 21525 (see [16]). So the coherent 6-sets yield all code words of weight 6 in $C^\perp$.

Also for some weights occurring in C the corresponding code words can be accounted for in a more theoretic way.

weight	number of code words
0,126	1
6,120	21525
8,118	1228500
10,116	184552200
12,114	18552581250
14,112	1314242167500
16,110	68079082765050
18,108	2667514596045250
20,106	81120550319953200
22,104	1954268046055820250
24,102	37924129974003107625
26,100	601068274770626079480
28, 98	7871132213541952114500
30, 96	86003428522692699669525
32, 94	790676681158633859233875

weight	number of code words
34,92	6160512966566502512146500
36,90	40933186152747536692851800
38,88	233196885552052675471341375
40,86	1144458561403784200188758850
42,84	4858299700266647804047008000
44,82	17902783039228562237737038750
46,80	57444582099852105080832400050
48,78	160926311556224375790588057000
50,76	394499358043598096283245023710
52,74	847905860048538708672443181000
54,72	1600414904256326262263020974000
56,70	2656273048882773962828716181475
58,68	3880761895373175524889157806000
60,66	4994562484553575572315539465400
62,64	5665434441759763029730883712375

Table 2: the weight distribution of the dual code $C^{\perp}$ of $\mathcal{H}(5)$.

7.1 Words of weight 50 and 76

The characteristic vector χ of the switching set S constructed in section 6 satisfies $A\chi \equiv \chi \pmod 2$. So χ is a code word of weight 50 in C_A and (if extended by one coordinate) also in C. Note that this means that we are in case 1 of Theorem 4.1. We saw that the stabilizer of S has order 40 and index 150 in the automorphism group $\mathrm{P\Gamma U}_3(25)_u$ of $\mathcal{H}'(5)$. This holds for each of the 126 descendants of $\mathcal{H}(5)$, leading to 18900 code words of weight 50. We claim that all these code words are distinct. Suppose that they are not; then it is possible to switch $\mathcal{H}'(5)$ extended by an isolated vertex such that another vertex becomes isolated while the subgraph induced by S remains regular of valency 13. Let $\{S', S''\}$, with $|S'| \leq |S''|$, be the corresponding partition of S. If switching does not change the degree, every vertex of S' is adjacent to precisely $|S''|/2$ vertices of S''. But the degree is 13 and therefore $|S''| = 26$ and S' induces a coclique of size 24 in $\mathcal{H}(5)$. Such a coclique cannot exist because of Cvetković' bound (see [7], Theorem 3.1). Thus we obtained all code words of weight 50. In other words, starting with S, the action of the full automorphism group of $\mathcal{H}(5)$ produces all 18900 code words of weight 50 in C. And of course the words of weight 76 are their complements.

It also follows that there are no other sets in $\mathcal{H}'(5)$ inducing a graph on 50 vertices of degree 13. Hence:

Theorem 7.1 *Up to isomorphism, there is only one* srg$(126, 50, 13, 24)$ *in* $\mathcal{H}(5)$.

7.2 Words of weight 52 and 74

Let A_u be the adjacency matrix of $\mathcal{H}'(5) \cup \{u\}$. Each non-zero row of A_u has weight 52, and so has the sum of any two rows of A_u corresponding to mutually non-adjacent vertices of $\mathcal{H}'(5)$. On the other hand the sum of any two rows of A_u corresponding to mutually adjacent vertices of $\mathcal{H}'(5)$ yields a code word of weight 74 in C, so its complement (which is also contained in C) has weight 52. Since $\mathcal{H}'(5)$ has 125 vertices and 7750 pairs of vertices, we obtain 7875 words of weight 52 in C. These words are all distinct. Indeed, if two such words would coincide, one would find a linear combination of four or less rows of A_u giving $\underline{0}$, contradicting the fact that $C^\perp$ has minimum weight six (see Table 7). Consequently a word of weight 52 in C is either a row of A_u, or the sum of two rows of A_u corresponding to mutually non-adjacent vertices of $\mathcal{H}'(5)$, or the complement of the sum of two rows of A_u corresponding to mutually adjacent vertices of $\mathcal{H}'(5)$. As the words of weight 74 are the complements of the words of weight 52, they can be deduced from this construction as well.

8 The Hoffman-Singleton graph

By use of the already mentioned description of $\mathcal{H}(5)$ in terms of the Hoffman-Singleton graph (for short HoSi), we can explain more about the two-graph code C of $\mathcal{H}(5)$. We recall a construction of HoSi based on the following well-known result.

Lemma 8.1 *There exists a bijective correspondence between the* 35 *lines of* PG(3, 2) *and the* 35 *unordered triples in a* 7*-set such that lines intersect if and only if the corresponding triples have exactly one element in common.*

The vertex set of HoSi consists of the 15 points and the 35 lines of PG(3, 2). Points are mutually non-adjacent; lines are mutually adjacent if and only if the corresponding triples are disjoint. A point is adjacent to a line if and only if they are incident in PG(3, 2). It is easily proved that HoSi is an srg $(50, 7, 0, 1)$. Several constructions and a proof of uniqueness can be found in [1].

Define a graph Φ' as follows: its vertices are the edges of HoSi, and two vertices are adjacent if and only if the corresponding edges of HoSi are at mutual distance two, i.e. are disjoint edges in a pentagon. It is easily proved that Φ' is an srg $(175, 72, 20, 36)$. Now fix a vertex u of HoSi and let F be the set of vertices at distance two from u. Then the subgraph $\Gamma(u)$ of Φ' induced by restriction of the vertex set to the set of edges of HoSi inside F is an srg $(126, 50, 13, 24)$. This is the mentioned construction of Goethals. It is known (see [17]) that the two-graph in which $\Gamma(u)$ is contained is $\mathcal{H}(5)$. We saw that the dimension of the code C of $\mathcal{H}(5)$ is 21, so by Theorem 4.1 the dimension of the code $C_{\Gamma(u)}$ of $\Gamma(u)$ is 20. Let Φ be the two-graph of which Φ'

weight	C_Γ	C_Φ
0,176	1	1
50,126	176	0
56,120	1100	1100
64,112	4125	4125
66,110	5600	0
70,106	17600	0
72,104	15400	15400
78, 98	193600	0
80, 96	604450	604450
82, 94	462000	0
86, 90	369600	0
88	847000	847000

Table 3: Weight distribution of C_Γ and C_Φ.

is a descendant. Since $\Gamma(u)$ is a subgraph of Φ', the Hermitian two-graph $\mathcal{H}(5)$ is a sub-two-graph of Φ.

Recall that the vertices of HoSi can be seen as the points and lines of $\mathrm{PG}(3,2)$; consequently the edges of HoSi, which correspond to the vertices of Φ', can be partitioned into a set of 105 edges between a point and a line and a set K of 70 edges between lines. Add an isolated point to Φ' and switch with respect to K. This yields an srg$(176,70,18,34)$ Γ in Φ. The code C_Γ of Γ is the 22-dimensional code discovered by Calderbank and Wales [3] (see also [8] and [13]). In this section we will construct the code C of $\mathcal{H}(5)$ from C_Γ. For this purpose we quote the weight enumerator of C_Γ from [3] in Table 8. We shall also need the fact that the 176 words of weight 50 in C_Γ make up the symmetric 2-$(176,50,14)$ design of G. Higman [11].

By Theorem 4.1 the two-graph code C_Φ of Φ is contained in C_Γ and has dimension 21. Since $n=176$ and the parameters $k=72$, $\lambda=20$ and $\mu=36$ of Φ' are divisible by 4, the codes $C_{\Phi'}$ of Φ' and C_Φ of Φ are self-orthogonal doubly even codes. A simple counting learns that the words of C_Φ are exactly the words of C_Γ which have a weight divisible by four (see Table 8). In fact, the code $C_{\Phi'}$ can also be described as the code generated the residual of Higman's design, see [13].

Lemma 8.2 *There exists a code word w of weight 50 in C_Γ such that the complement of w is the characteristic vector of the vertex set of $\Gamma(u)$.*

Proof. Consider a partition of the vertex set of HoSi into points and lines of $\mathrm{PG}(3,2)$ and the corresponding partition of the vertex set of Φ' into a set of 105 edges of HoSi between a point and a line and a set K of 70 edges of HoSi between lines. Fix a vertex u of HoSi which corresponds to a point of $\mathrm{PG}(3,2)$. Then the set F of 42 vertices of HoSi at distance two from u can be partitioned into a set of 14 points and a set of 28 lines. The 126 edges inside F induce the subgraph $\Gamma(u)$ of Φ'. The vertex set of $\Gamma(u)$ can be partitioned into a set L of 84 edges of HoSi between a point and a line and a set of 42 edges of HoSi between lines. Add an isolated point ∞ to Φ' and switch with respect to K. Then one obtains the graph Γ. It is straightforward to check that the rows of the adjacency matrix of Γ corresponding to L and ∞ add up to a code word $\overline{w}$ of weight 126 which is the characteristic vector of the vertex set of $\Gamma(u)$. Since $\underline{1} \in C_\Gamma$, the complement w of $\overline{w}$ is also a code word of C_Γ. $\square$

Consider any two distinct code words x and y of C_Φ and suppose that after deleting the 50 coordinate positions corresponding to the ones in the word w from Lemma 8.2 they would be the same. Then $x+y$ would be a non-zero code word of C_Φ of weight at most 50, contradicting the fact that C_Φ has minimum weight 56. So distinct code words of C_Φ remain distinct after deleting the 50 coordinate positions corresponding to the ones in w. As C and C_Φ have the same dimension, it follows that C can be obtained from C_Φ by deleting the 50 coordinate positions supported by w.

Thanks to this description of C we can understand better some facts about the weight enumerator.

Proposition 8.3 *The code C of the Hermitian two-graph $\mathcal{H}(5)$ has minimum weight at least* 36*.*

Proof. Let w be the word of weight 50 constructed in Lemma 8.2 and let x be a non-zero code word of C_Φ of weight $a+b$, where a denotes the number of common ones of w and x. Then x yields a word of weight b in C. We must show that $b \geq 36$. We know that $a+b$ is at least 56 and divisible by 4. The word $y = w + x$ is a word of weight $50 - a + b$ in C_Γ which is not in C_Φ. Therefore the weight of y is at least 50 and not divisible by four, hence $b - a$ is non-negative and divisible by 4. Suppose the weight of y is 50. We saw that the words of weight 50 in C_Γ form a symmetric 2-$(176, 50, 14)$ design. Any two blocks of such a design meet in 14 points, so $a = 36$ and $b = 36$. Otherwise the weight of y is at least 66, which implies that $b \geq 36$. $\square$

8.1 Words of weight 36 and 90

Fix a vertex u in HoSi, let F be the set of 42 vertices at distance two from u, and let D be the set of 7 vertices adjacent to u. Pick a vertex v in D. Then F can be partitioned into a set Y of 6 vertices adjacent to v and a set Z of 36 vertices at distance two from v. The 126 edges inside F can be partitioned into 36 edges from Y to Z and 90 edges inside Z (note that Y is a coclique). So a partition of the vertex set of $\Gamma(u)$ into a 36-set and a 90-set arises. With the help of Lemma 3.1, the corresponding partition of the adjacency matrix of $\Gamma(u)$ is easily seen to be regular with quotient matrix

$$\begin{bmatrix} 5 & 45 \\ 18 & 32 \end{bmatrix}.$$

By summing the rows corresponding to one set of the partition a code word of weight 36 in C is obtained. Using the computer package GAP [5] and the share package Projective Geometries [4] for GAP written by J. De Beule, P. Govaerts and L. Storme, we checked that the action of the automorphism group of $\mathcal{H}(5)$ produces all 525 code words of weight 36. The code words of weight 90 are the complements of those of weight 36.

8.2 Words of weight 42 and 84

Consider the partition of the vertex set of HoSi into the 15 points and 35 lines of $\mathrm{PG}(3,2)$, respectively, and let u be a point of $\mathrm{PG}(3,2)$. Then the set F of 42 vertices at distance two from u consists of 14 points and 28 lines. The edges inside F can be partitioned into 84 edges between a point and a line and 42 edges between lines (note that points are mutually non-adjacent), so a partition of the vertex set of $\Gamma(u)$ into a 42-set and an 84-set is obtained. The corresponding partition is easily proved to be regular with quotient matrix

$$\begin{bmatrix} 8 & 42 \\ 21 & 29 \end{bmatrix}.$$

Summing of the rows corresponding to one set of the partition yields a code word of weight 84 in C. Again we used GAP [5] and Projective Geometries [4] to check that all 2250 code words of weight 84 can be obtained from this one by the action of the automorphism group of $\mathcal{H}(5)$. The words of weight 42 are the complements of those of weight 84.

Acknowledgements. We thank Ted Spence for generating by computer all possible switching sets S in $\mathcal{H}'(5)$. This enabled us to find the explicit description of S given in Section 6, and it confirmed the result of Theorem 7.1. We also thank Jan De Beule for his help with GAP and Projective Geometries.

References

[1] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin, 1989.

[2] A. E. Brouwer, H. A. Wilbrink and W. H. Haemers, Some 2-ranks, *Discrete Math.* 106-107: 83-92 (1992). A collection of contributions in honour of Jack van Lint.

[3] A. R. Calderbank and D. B. Wales, A global code invariant under the Higman-Sims group, *J. Algebra* 75: 233-260 (1982).

[4] J. De Beule, P. Govaerts and L. Storme, Projective Geometries, a share package for GAP (2000), `http://cage.rug.ac.be/~jdebeule/pg`.

[5] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.2 (2000), `http://www.gap-system.org`.

[6] J.-M. Goethals and J. J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* 12: 143-158 (1975).

[7] W. H. Haemers, Interlacing eigenvalues and graphs, *Linear Algebra Appl.* 226-228: 593-616 (1995).

[8] W. H. Haemers, C. Parker, V. Pless and V. D. Tonchev, A design and a code invariant under the simple group Co_3, *J. Combin. Theory Ser. A* 62: 225-233 (1993).

[9] W. H. Haemers, R. Peeters and J. M. van Rijckevorsel, Binary codes of strongly regular graphs, *Des. Codes Cryptogr.* 17: 187-209 (1999).

[10] W. H. Haemers and V. D. Tonchev, Spreads in Strongly Regular Graphs, *Des. Codes Cryptogr.* 8: 145-157 (1996).

[11] G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* 13: 74-80 (1969).

[12] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* 32: 418-443 (1974).

[13] C. Parker and V. D. Tonchev, Linear codes and doubly transitive symmetric designs, *Linear Algebra Appl.* 226-228: 237-246 (1995).

[14] J. J. Seidel, Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3, *Linear Algebra Appl.* 1: 281-298 (1968).

[15] J. J. Seidel, A survey of two-graphs, Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), *Atti dei Convegni Lincei* 17 Tomo I: 481-511 (1976).

[16] E. Spence, Is Taylor's graph geometric?, *Discrete Math.* 106-107: 449-454 (1992). A collection of contributions in honour of Jack van Lint.

[17] D. E. Taylor, Some topics in the theory of finite groups, Ph. D. Thesis, Univ. Oxford, 1971.

[18] D. E. Taylor, Regular 2-graphs, *Proc. London Math. Soc.(3)* 35: 257-274 (1977).